



# **HOMELAND SECURITY 2002:**

## **EVOLVING THE HOMELAND DEFENSE INFRASTRUCTURE**

# **EXECUTIVE SUMMARY REPORT**

September 2002

*(Conference Proceedings — June 25 - 26, 2002)*

Volume 1, No. 2

Renaissance Washington DC Hotel

[www.e-gov.com](http://www.e-gov.com)

REPORT DOCUMENTATION PAGE			Form Approved OMB No. 074-0188	
Public reporting burden for this collection of information is estimated to average 1 hour per response, including the time for reviewing instructions, searching existing data sources, gathering and maintaining the data needed, and completing and reviewing this collection of information. Send comments regarding this burden estimate or any other aspect of this collection of information, including suggestions for reducing this burden to Washington Headquarters Services, Directorate for Information Operations and Reports, 1215 Jefferson Davis Highway, Suite 1204, Arlington, VA 22202-4302, and to the Office of Management and Budget, Paperwork Reduction Project (0704-0188), Washington, DC 20503				
1. AGENCY USE ONLY (Leave blank)		2. REPORT DATE 9/1/2002	3. REPORT TYPE AND DATES COVERED Report 9/1/2002	
4. TITLE AND SUBTITLE Homeland Security 2002: Evolving the Homeland Defense Infrastructure Executive Summary Report			5. FUNDING NUMBERS	
6. AUTHOR(S) McGrath, Martha W.; Randolph, Terri; Lamont, Judith; Dervarics, Charles J.				
7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)  Egov			8. PERFORMING ORGANIZATION REPORT NUMBER	
9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)			10. SPONSORING / MONITORING AGENCY REPORT NUMBER	
11. SUPPLEMENTARY NOTES				
12a. DISTRIBUTION / AVAILABILITY STATEMENT Approved for public release; distribution is unlimited			12b. DISTRIBUTION CODE  A	
13. ABSTRACT (Maximum 200 Words)  The second E-Gov Homeland Security 2002 Conference was held June 25-26 in conjunction with the E-Gov 2002 Exposition in Washington, DC. The conference was focused on Evolving the Homeland Defense Infrastructure, and addressed the current policy and technology-related issues for ensuring our national homeland security. Sessions were organized into two tracks: 1) Creating an Infrastructure for Homeland Security and 2) Building Integrated Homeland Security Operations. Conference participants recognized the overriding importance of cultural change in developing effective				
14. SUBJECT TERMS IATAC Collection, homeland security			15. NUMBER OF PAGES  39	
			16. PRICE CODE	
17. SECURITY CLASSIFICATION OF REPORT UNCLASSIFIED	18. SECURITY CLASSIFICATION OF THIS PAGE UNCLASSIFIED	19. SECURITY CLASSIFICATION OF ABSTRACT UNCLASSIFIED	20. LIMITATION OF ABSTRACT  UNLIMITED	

# **HOMELAND SECURITY 2002: EVOLVING THE HOMELAND DEFENSE INFRASTRUCTURE**

---


**June 25 - 26, 2002  
Renaissance Washington DC Hotel  
Washington, DC**

---

**Published by:**



**A 101communications Company**

Homeland Security 2002: Evolving the Homeland Defense Infrastructure  
is an  Conference.

**[www.e-gov.com](http://www.e-gov.com)**

## Homeland Security 2002 Executive Summary Report

**Conference Chairman**  
Michael J. Mestrovich, Ph.D.

**Editor**  
Martha W. McGrath  
martha@e-gov.com

**Assistant Editor**  
Terri Randolph  
terri@e-gov.com

**Senior Writers**  
Judith Lamont  
jlamont@sprintmail.com  
Charles J. Dervarics  
dervarics@cs.com

**Copy Editors**  
Pat Beezley  
pat@e-gov.com  
Steven J. Smith  
steve@e-gov.com

**Graphic Designer**  
Sharon Lill

Conference Overview .....	5
Agenda .....	6
Conference Keynotes .....	8
Plenary Session 1: <i>Homeland Security Programs — The First Wave</i> .....	16
Track 1: <i>Creating An Infrastructure For Homeland Security</i> .....	18
Track 2: <i>Building Integrated Homeland Security Operations</i> .....	24
Plenary Session 2: <i>Attendee Discussion Forum: Technologies and Strategies for HLS — Today and Tomorrow</i> .....	32
Summary of Attendee Recommendations and Questions .....	34
Conference Sponsor Profiles .....	36



The second E-Gov Homeland Security 2002 Conference was held June 25-26 in conjunction with the E-Gov 2002 Exposition in Washington, DC. The conference was focused on Evolving the Homeland Defense Infrastructure, and addressed the current policy and technology-related issues for ensuring our national homeland security. Sessions were organized into two tracks: 1) Creating an Infrastructure for Homeland Security and 2) Building Integrated Homeland Security Operations.

Conference participants recognized the overriding importance of cultural change in developing effective homeland security programs. Political and organizational challenges present greater barriers to sharing information than do technological limitations. Speakers cited examples of improved cooperation, but acknowledged that many turf battles are still being fought, and that deeply entrenched organizational structures and processes have proven resistant to change.

Many speakers pointed to the need for building solid relationships in advance, so they are in place when an emergency arises. Open communication and trust among diverse professionals cannot be developed in the throes of a crisis; rather, they require time and exchange of ideas to develop. These kinds of organizational relationships also pave the way for better implementation of technology for homeland security initiatives. The federal government has 55 databases that deal with security threats, but inter-agency access depends on establishing agreements through which that information can be shared. True cooperation also will require government-wide commitment to enterprise architecture, integrated information systems, and interoperable communication systems.

Conference attendees emphasized a need to move beyond philosophical discussions into a review of demonstrated homeland security solutions at the organizational and technological levels. High on the list of practical concerns was the issue of how to fund these initiatives. The economic downturn has sharply decreased the resources available to state and local governments at a time when more demands are being placed upon them. An urgent need also is felt by local jurisdictions for prioritizing and benchmarking of security measures what steps are most important, and how will government entities know when they have achieved an acceptable level of protection? They are looking to the federal government for best practices, guidelines, and recommendations for action.

In closing the conference, discussion centered on the dynamic tension between freedom versus security — perhaps the one philosophical issue that remained at the forefront. Although the events of 9/11/01 forced a re-evaluation of this balance, many attendees remained reluctant to endorse a widespread change in the fabric of American society. Lively discussions ensued regarding the possibility of issuing national identity cards, enforcement of border security, and the treatment of visiting foreign students. Participants viewed this topic—what kind of society do we want to create and live in—as warranting a continued and serious dialogue in the context of future homeland security.



## Homeland Security 2002: Evolving the Homeland Defense Infrastructure

June 25 - 26, 2002  
Renaissance Washington DC Hotel  
Washington, DC

### Tuesday, June 25, 2002

8:15am

Welcome and Opening Remarks

8:30

**Opening Keynote:** Patrick Schambach  
Associate Under Secretary and CIO/CTO  
Transportation Security Administration



9:45

**Plenary Session 1:** Homeland Security Programs - The First Wave

11:15

**Session 1-1:** Evolving Towards a Culture of Cooperation

**Session 2-1:** Organizational Constructs That Work

12:30pm

**Featured Speaker and E-Gov 2002 Awards Luncheon:** Jim Flyzik, Senior Advisor to Governor Tom Ridge, Office of Homeland Security

2:45

**Session 1-2:** Maximizing Resources for E-Government and Homeland Security Integration

**Session 2-2:** Securing the Transportation Infrastructure

4:00

**Session 1-3:** Securing Public Health Services - A Cross-Jurisdictional Approach

**Session 2-3:** Technology at the Border

5:00

Conference Reception

# Homeland Security 2002: Evolving the Homeland Defense Infrastructure

June 25 - 26, 2002  
Renaissance Washington DC Hotel  
Washington, DC

## Wednesday, June 26, 2002

**8:45am**

**Opening Keynote:** Rudolph Giuliani, Former Mayor, New York City

**10:00am - 5:00pm**

E-Gov 2002 Exposition and Homeland Security Pavilion

**12:00noon**

**Luncheon Keynote:** David Tubbs, Former Executive Director  
Utah Public Safety Command and Director 2002 Winter Olympics Security

**1:30pm**

**Session 1-4:** Translating Technologies into Capabilities

**Session 2-4:** Technology Priorities for State and Local  
Governments

**2:45**

**Session 1-5:** Information Assurance - Integration with  
HLS Solutions

**Session 2-5:** Industry Preview - What's Over the Horizon

**4:00**

**Plenary Session 2:** Attendee Discussion Forum:  
Technologies & Strategies  
for HLS - Today and Tomorrow

**5:00**

**Adjourn**



*Ron Miller, Chief Information Officer, FEMA*





**Patrick Schambach**  
Associate Under Secretary and CIO/CTO  
Transportation Security Administration

### ***Taking Steps Toward Homeland Security at TSA***

Mr. Schambach provided a comprehensive look at the Transportation Security Administration (TSA), which was created by PL 107-71 in November 2001 as part of the government's response to the events of 9/11/01. Its mission is to protect the nation's transportation systems to ensure freedom of movement for people and commerce. TSA began exploring U.S. transportation vulnerabilities in light of the new set of threats posed by terrorists. Discussions held during meetings of the Interagency Technical Support Working Group (ITSWG) helped to highlight some of the reasons these threats are so difficult to counter, including the prevalence of global travel, availability of information technology that allows terrorists to communicate, the ease of obtaining materials for weapons, and the willingness of terrorists to die in attacks. To meet these challenges, TSA operates under three basic premises:

- **Identify critical priorities:** "You can't protect everything at the same level," said Mr. Schambach. "Security is all about balance."
- **Increase information sharing:** Key players and agencies must share intelligence as well as preparation plans and lessons learned from past experiences.
- **Improve analysis:** The federal government needs to upgrade data analysis and warning capabilities. Overall, faster response rates are essential.

The major focus for TSA has been aviation security, to develop improved methods of screening passengers, airport personnel, baggage, and cargo. In addition, aircraft security and airport perimeter security have been identified as top priorities. Mr. Schambach pointed out that TSA has a daunting mandate: ensuring secure operations at more than 400 commercial airports nationwide that move more than two million passengers and several hundred thousand checked bags per day. According to present legislation, procedures must be in place by the end of December 2002 to screen 100% of checked baggage. Meeting these goals will require TSA to hire and train a staff of approximately 30,000 passenger screeners and 21,000 additional baggage screeners.

**"You can't protect everything at the same level. Security is all about balance."**

TSA is developing what Mr. Schambach described as a "passenger-centric" process to control the flow of people through airports. Schambach envisions a policy of "smart screening" in which all passengers receive a basic security check with additional checkpoints for those not recognized as "trusted travelers."



The supporting technology will include options for using a variety of devices, including desktop and laptop computers, personal digital assistants, and other communication devices. In developing the architecture, TSA will begin with a business strategy and implement the necessary technology to support it. In order to be effective, the system must be web-enabled and connect departments within TSA as well as other organizations, including the FBI, CIA, NSA, State Department, INS, Office of Homeland Security, and selected foreign airports and carriers. Among aviation and security experts, he said, “there’s a tremendous willingness to share as never before.”

In the “red, white, and blue” plan for phasing in the system, “red” will provide initial operating capability, “white” will add functionality, and “blue” will deploy the final end-to-end system and comprehensive operational procedures. Each phase will build upon the previous one. Outsourcing will be used as much as possible, said Mr. Schambach, relying on the combined expertise of the public and private sectors. His goal is to have one vendor who will manage all of the services. Outsourcing also will allow evolution of the system without requiring new capital investment from the government. Evaluation of the system’s effectiveness will focus on mission results, while keeping the traditional information technology metrics in place.

More changes are expected by the end of 2002, particularly with the December 31 deadline to implement a new explosive detection system for checked baggage. Other improvements are likely to include:

- **New walk-through metal detectors, with first-time certification standards:** Among the advanced screening equipment to be deployed is x-ray technology in which a threat will be superimposed over the bag being inspected, requiring a “yes” or “no” response from the screener. Since only one in a million bags will contain an actual threat, it is difficult for the screeners to remain vigilant; a design that includes a requirement for a response helps focus the screener’s attention.
- **New x-ray technology for carry-on bags:** New walk-through metal detectors are being installed and there now is a common standard for setting the sensitivity level, in response to past criticism of inconsistency across different airports.
- **A new credentialing system for airline employees:** Each of whom will receive a Transportation Worker Identification Card, or TWIC.

Mr. Schambach concluded by reiterating the need for support from the private sector, and inviting interested companies to contact TSA with their recommendations. Referring to a speech in which President Bush cautioned Americans that we are facing people who “hate our existence,” he underscored the urgency of reducing vulnerabilities in aviation transportation.





**Jim Flyzik**  
Senior Advisor to Governor Tom Ridge  
Office of Homeland Security

### ***Our Shared Responsibility for Homeland Security***

Mr. Flyzik provided insights about the goals and structure of the newly-authorized Office of Homeland Security (OHS). Flyzik called this undertaking “the most ambitious reorganization” of federal agencies in more than 50 years. To give an idea of the magnitude of this initiative, he compared it to executing a \$37 billion corporate merger. On the one hand, the office is a new organization with a new mission, yet it also must integrate the functions and personnel of numerous existing organizations.

For its part, the Bush Administration has two clear priorities in homeland security: 1) to prevent attacks, and 2) to minimize damages if prevention efforts fail. He emphasized that Homeland Security is “a national effort, not a federal effort,” that will involve organizations at all levels across government. “The homeland will be secure when the hometown is secure,” Flyzik observed. “We want to ensure that threat information gets to the state and local levels,” he added.

Many agencies already are spending considerable funding on efforts to thwart terrorists. Given these substantial investments, it is important to make the most of them through consolidation and by leveraging each dollar to yield the maximum benefits.

The OHS plan is for the new agency to absorb diverse organizations from the Coast Guard, Secret Service, Federal Emergency Management Agency, Immigration and Naturalization Service, Customs Service, General Services Administration, and others. It will be composed of four divisions each headed by an Under Secretary. The divisions are:

- Border and Transportation Security
- Emergency Preparedness and Response
- Chemical, Biological, Radiological, and Nuclear Countermeasures
- Information Analysis and Infrastructure Protection

**“The homeland will be  
secure when the  
hometown is secure,”  
Flyzik observed.**

“We know that we cannot connect every computer together, and that there will be risks,” according to Flyzik. Yet from a technology standpoint, the major goal is to create a systems environment that supports information-sharing and appropriate access. To that end, a high priority is to tear down federal information “stovepipes” and move to a more integrated system that allows for more coordinated efforts and streamlined communications.

One major vehicle for this new approach involves the Critical Infrastructure Assurance Office (CIAO) plans to form an Information Integration Program Office as chartered by the Homeland Security Council. Goals for this office are to develop an architected environment for information-sharing with two primary themes: improved access to federal databases and increased capacity to share threat information with local officials. The goal of these efforts, Flyzik remarked, is “peer-to-peer communication among partners,” not a top-down emphasis to information development and sharing.

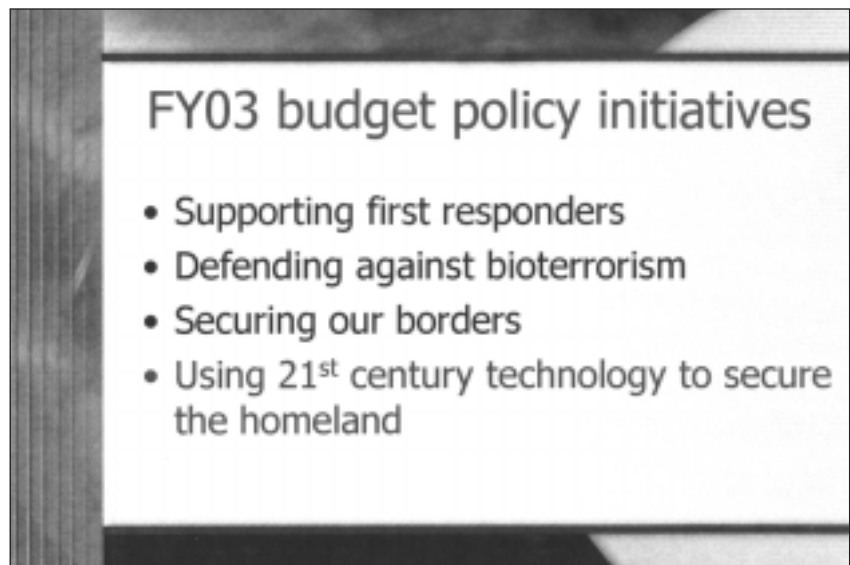
OHS will establish two types of projects: (1) foundation projects that will take place over the next six to nine months and will be implemented by federal agencies to produce business and information architectures, and (2) pilot projects that have a 24-month time frame but are designed to produce tangible value in 90 days. The pilot projects include watchlist consolidation among several different agencies and a Homeland Security portal.

Other initiatives will play important roles in enhancing homeland security. The Critical Infrastructure Protection Board, for example, is geared toward defending cyberspace, establishing a wireless priority access system, and new firewall projects to protect the integrity of federal computer systems and networks. Coordination,

collaboration, and communication with other government organizations is being improved by working with groups such as the National League of Cities, National Association of Counties, and U.S. Conference of Mayors.

To date, the Administration’s coordinated anti-terrorism activities have brought together experts from the military, intelligence communities and health care, among others. Flyzik said the nation will reap benefits from this new level of cooperation. Going forward, the federal budget will include funding for training and supporting first responders and for fighting bioterror.

“Security investments improve public health and commerce,” according to Flyzik, and they lead to better communication across federal, state, and local agencies. “We don’t pretend to know this all by ourselves,” he added.



Source: Jim Flyzik briefing 6/25/02.



**Rudolph Giuliani**  
Former Mayor of New York City

### *Leadership in Difficult Times*

Preceded by two bagpipers, former New York City Mayor Rudolph Giuliani took the stage with a blend of inspiring guidance and pragmatic advice. He began by highlighting the natural partnership and importance of viewing E-Government and Homeland Security as separate initiatives with similar goals. Former Mayor Giuliani said that this partnership will allow us to understand the risks and be prepared, while still leading productive lives. If we do not move forward, he said, the terrorists will have accomplished their goal.

Although many people view the world as a more dangerous place now, Mr. Giuliani's perspective is just the opposite. All the risks were there a year ago, he pointed out, but we did not see them. The philosophy that was behind the attacks was already in play. The only difference now is that the curtain preventing us from seeing the world as it really was has been lifted. Those who wish our destruction because they believe our society is flawed attacked us for what is right about our society—the rule of law and respect for human value. The danger is there, and will be for some time.

"We have to confront the dangers that exist, and the moment you confront reality, you're safer," he said. We are doing the right things overseas to protect American interests abroad, and we will do the same at home. Mr. Giuliani emphasized that even as we warn and plan, we also must relax and enjoy life. Although we will find the new path challenging, greater risks have been confronted by this and other countries in the not-so-distant past. He recalled the difficulties faced by the English people during World War II when their country was bombed daily. The problems we have now are difficult too, but not unprecedented.

Mr. Giuliani then shifted his focus to how technology and good management helped New York City identify and resolve a number of social and economic problems while he was in office. Crime was rampant, a majority of people wanted to move out of the city, and the government budget was running a deficit. The city was viewed as "unmanageable" and "ungovernable," which became an excuse for "unaccountability." This was the primary assumption that Mayor Giuliani set out to change.

Tackling crime first, the Mayor's office identified an immediate need for current statistics on where most crime was occurring. Law enforcement pinmapped crime locations to see how they clustered, and then plotted them against the time of day. The police department met to discuss crimes, and the precinct

---

**The only difference now  
is that the curtain  
preventing us from  
seeing the world as it  
really was has been lifted.**

commanders were made accountable. Resources were allocated where they most were needed, with a resulting decrease in crime citywide.

A similar philosophical change took place in the city's welfare system, which initially had more than a million individuals enrolled from a city population of 7 million. Rather than define success as enabling people to receive welfare, a program was organized around helping this population find jobs. The welfare office was renamed the NYC Job Center to demonstrate this new approach. Similarly, creative methods were used to find children who were eligible for, but not enrolled in, public health care programs. Various city agencies, including the police and fire departments, were taught how to identify children and families who were qualified for the program benefits, which ultimately served to reach approximately half of those who previously were without coverage or adequate health care.

The 1993 bombing attack on the World Trade Center increased awareness of the potential terrorist threat, and in 1996, Mayor Giuliani's office created a municipal Emergency Management System. Its purpose was to modernize plans for dealing with emergencies, including chemical and biological terrorist attacks, and to create a coordinating agency. The office divided its time between coordinating current emergencies, and planning and drilling for future events.

The drills were virtual computer simulations and physical street exercises, and some embodied an almost eerie foreshadowing of later events. For example, one was a simulated attack four blocks from the World Trade Center, of a sarin gas attack involving 5,000 people. Another was a plane crash in Queens on the border of Manhattan and was designed to test coordination among the boroughs. There were times, said Mr. Giuliani, that people on the teams resented the Saturday mornings devoted to the drills and wondered about their usefulness.

This skepticism came to an end abruptly on the morning of September 11, 2001. At first, when he saw people jumping out of the windows of the World Trade Center, then-Mayor Giuliani reflected that they did not have a plan for this scenario. "I thought we would have to make it up as we went along," he said. His team felt initially unprepared, but as the morning went on and they made decisions, such as getting air cover, generators, and FBI agents to secure the city, he realized that prior exercises and preparations were relevant, although this tragic situation was on a much larger scale than previously anticipated. The advance work helped NYC officials to save lives, as well as create more calm among the public, however traumatized.

Mr. Giuliani closed his speech by recognizing the importance of having a positive relationship between the government and its citizens. By using technology, government can make routine activities easier for citizens. Whether a citizen is paying a parking ticket or opening a restaurant, E-Government efforts can assist by removing the need to understand the entire bureaucracy. Moving these activities online also helps make government accountable because performance measures can be readily developed and distributed. "People should have a confident relationship with government," he said. "E-Government can go a long way toward accomplishing that."

Today's world requires a greater focus on security, but if the government does its job in providing such security, people can go about their lives. Mr. Giuliani believes the United States has handled this challenge well. We face many difficulties besides terrorism, and need to keep a sense of perspective. America is still the most vital society in the world, and, he pointed out, it is still the place that everyone wants to come to. "Terrorists cannot take away our freedom unless we do it for them," concluded Giuliani.





**David Tubbs**

**Former Executive Director, Utah Public Safety Command,  
and Director 2002 Winter Olympics Security**

***Applying Lessons Learned: Securing the  
2002 Winter Olympic Games***

Mr. Tubbs discussed the procedures and lessons learned from his experience managing for the 2002 Winter Olympics, specifically as they relate to the future of national homeland security initiatives. Even before last September, he said, security was a major concern at an event that involved 3,500 athletes attending 140 ticketed events at 10 venues across the Salt Lake City area. The 2002 Winter Olympics were viewed by many as a test of whether the United States could effectively prevent terrorism from disrupting such a high-profile, international event. Many questions were raised about how those responsible for security during the Winter Olympic Games could protect an area covering 900 square miles, with 70,000 visitors a day, 18,000 volunteers, and 9,000 accredited members of the media.

Planning and communication were central to the success of security at the Olympics, said Mr. Tubbs. More than 20 organizations, including law enforcement, fire protection, and emergency management services, in the Utah Public Safety Command, served as a central clearinghouse for debate, discussion, and coordination. “Without one committee, you won’t get the job done,” he said.

Public safety personnel from the State of Utah conducted joint planning, training, gap analysis, and consequence management. Federal partners provided additional resources to fill in identified gaps. Tubbs also brought in public health officials and sophisticated equipment to monitor for chemical and biological hazards. Due to this planning and communication, everyone knew where they fit into the security architecture for the Olympic Games. All members of the team had access to relevant security information, with special clearances arranged for state and local personnel so they could be fully informed. Channels of communication also were established with the media before the events began.

The Olympics Security team took a number of steps to foster public confidence. Public safety staff were clearly identified with yellow coats labeled “Police,” and the National Guard presence also was visible. Although there were some initial concerns that visitors might react negatively to armed security, spectators in fact approached the Guard personnel and thanked them for being there. Since security concerns covered not just terrorism but also criminal activity, corrections officials were in place to identify and extract parolees who might represent a public threat.

**Planning and  
communication were  
central to the success of  
security at the Olympics.**

The security process was marked by vigilance on many fronts. To help protect communications, cameras were placed on microwave towers. At one point, snowmobilers approached the towers too closely, and Blackhawk helicopters were on the scene in less than two minutes. No overflights of the Olympic venues were allowed, and inbound aircraft had to stop at one of six regional airports before being cleared to land at Salt Lake City. About 600 bomb threats were received, but no negative incidents occurred.


Fortunately, because of the care taken in planning and managing the operations for the 2002 Winter Olympics, the games proceeded smoothly. Mr. Tubbs was pleased to report that the worst problem encountered was traffic congestion. He attributes the overall success to a number of factors, but particularly to careful relationship-building prior to the Olympics and to links created ahead of time among different agencies. Personnel and media were kept informed of developments as they happened, reducing chances of confusion or misunderstanding. Finally, resources were obtained and dedicated to the activities where they were most needed.

Overall, security costs totaled more than \$300 million, which included technology, staff salaries, and help from federal agencies. In assessing the success of the effort, Tubbs offered these suggestions for securing future events:

- **Plan carefully:** Tubbs conducted three large-scale simulations involving 1,000 individuals plus dozens of exercises with smaller groups. These were helpful in assessing security gaps, but he cautioned against over-planning. “Planning can be the end product if you’re not careful.”

- **Solicit local input:** Tubbs involved local and county agencies, securing top secret security clearances for the leadership to enable their participation in exercises and planning efforts. In the end, all police personnel—regardless of agency—wore yellow coats so they were easily identified in public. The security detail eventually included 2,400 Utah officers, 2,100 Federal officers under the direction of the Secret Service, 1,400 FBI agents, and 650 law enforcement volunteers from 48 states.

- **Work with the media:** The security office conducted twice-a-day media briefings to develop working relationships with reporters. This philosophy was particularly helpful after a false positive test for anthrax at a local airport. Tubbs brought in a public health official to conduct a media briefing immediately. “We didn’t want to be accused of covering anything up,” he said. “There’s no more ‘no comment.’”



## Top Ten List

(Things you may want to do)

- Identify a member of your agency to monitor Homeland Security related activities
- Assess current resources
- Anticipate and project potential costs to your agency
- Plan for situations and activities that may occur in your community
- Develop a media plan
- Intelligence
- Training and Equipment Issues
- Keep your personnel informed
- Create communication links with the other local, state, and federal Public Safety Agencies
- Build relationships!

Source: David Tubbs briefing 6/26/02.



## *Plenary Session 1: Homeland Security Programs - The First Wave*

### **Moderator:**

**Jerry Mechling, Ph.D.**, Director, Strategic Computing and Telecommunications in the Public Sector  
John F. Kennedy School, Harvard University

### **Panelists:**

**Raymond F. Geoffroy**, Assistant Deputy Commandant for Plans, Policies and Operations and  
Director Security Division, U.S. Marine Corps

**Matt Lampe**, Director, Strategic Planning, Department of Information Technology,  
City of Seattle, Washington

**Ron Miller**, Chief Information Officer, Federal Emergency Management Agency

**Richard Morris**, Advisor to the Director, Office of Public Health Preparedness  
Department of Health and Human Services

This panel examined how resources have been allocated during the first wave of response following 9/11/01, with perspectives provided from military, local, and federal viewpoints. Emerging themes are:

- More plans than actions have taken place, but this is not surprising considering the magnitude of the effort and the size and number of organizations involved.
- Cultural change, rather than technology, represents the biggest challenge. The panel reinforced a conclusion that technology would enable, but not define, long-term homeland security solutions.
- Key technology issues are data-sharing and security. Sharing information, creating secure communications, and providing effective analysis are among the most critical.

Dr. Jerry Mechling opened the session by describing the Harvard University program that has, since 1987, looked at how information technologies are being used throughout government, with particular focus on how to get senior program and political officials to work with senior technology officials to understand and take action on important activities. A year ago, there were a lot of investments being planned that did not consider a world where the foremost thing on our minds would be homeland security. Nor did we have to confront the fact that the economy is quite different than it was a year ago. We now have a new set of challenges, not only to respond to what has happened, but to do it in a governmental context where these activities to some degree have to reprioritize and reframe previous plans.

**Cultural change, rather than technology, represents the biggest challenge.**

Mr. Raymond Geoffroy discussed how the Marine Corps has begun to establish a role in homeland security by forming a Public Safety Division that includes a Homeland Defense Branch, a Critical Infrastructure Assurance Branch, and a Security and Law Enforcement Branch. The overall objective is to build partnerships to handle chemical and biological terror detection and monitoring. This is part of the Marines' "triad" approach for homeland security, that includes the 4th Marine Expeditionary Brigade (bringing together the chemical and biological response force with the Marine Corp security forces), USMC installations (first-responder communities) and reserve units (forces located outside the installations). Camp LeJeune is the first installation to fully implement a partnership and currently is exploring response options in the event of an attack.

Mr. Matt Lampe brought a local government viewpoint to the panel as he described the City of Seattle's handling of a range of emergency situations and a current assessment of its homeland security needs in light of those experiences. One issue he focused on was the pressing need for an 800 MHz standard for emergency communications, following years of struggle with the FCC on spectrum management. In addition, he noted that no standard of due care or model of responsibility has been defined for local protection. In this respect, he said, we are in much the same position as we were regarding environmental protection in the 1960s—aware of serious problems but without specific guidance. Seattle's present efforts include devoting \$235M to protect the city's reservoirs, establishing a new bureau for emergencies, increasing knowledge about how to maintain business continuity in the event of an emergency, and establishing a streamlined citywide IT program.



*Jerry Mechling, Raymond Geoffroy, Richard Morris, Ron Miller, and Matt Lampe.*

FEMA's Chief Information Officer, Mr. Ron Miller, began by noting that all disasters are local. To provide meaningful help to disaster victims, federal emergency staff must work effectively with local organizations. FEMA's role in responding to terrorism is not new, but was a part of its charter when the organization was formed in 1979. He believes that presently, too many initiatives are being activated without enough resources or integration. A better approach would be to determine the capabilities of each organization and establish an authorized organization in each major business area. To improve customer service for disaster victims, FEMA is developing [disasterhelp.gov](http://disasterhelp.gov), a website for people to go to directly for the services they need without negotiating the bureaucracy. Another initiative is Project SAFECOM, a government-to-government connection that relies on wireless technologies. SAFECOM would have full operability nationwide and include a homeland security advisory system to help governments collectively provide basic emergency services when and where disaster strikes.

The Department of Health and Human Services has established the Office of Public Health Preparedness (OPHP) to serve as liaison with the Office of Homeland Security, to advise the HHS Secretary on protection of the civilian population, and serve as the focus for state and local protection and response. Mr. Richard Morris said that state and local governments can receive grants that will assist them to provide stronger disease surveillance and improve hospital preparedness. Benchmarks of particular concern to OPHP are a 24/7 communications system, the ability to deliver vaccines and antibiotics within three to five days to large populations, and the ability of hospitals to respond to surges in demand of over 500 acutely ill patients at one time. On the information technology side, OPHP seeks to ensure that 90% of the population has Internet connectivity to keep the public informed in the event of biological attack or an epidemic due to infectious disease.

Dr. Mechling concluded the session by remarking "A year ago, E-Government was moving from what we did in the past, which was largely taking our services and putting them out there one program at a time, to the integration, or 'cross boundary' agenda." He noted that our collective security concerns have raised the demands for information-sharing that crosses jurisdictional boundaries. "That's the good news," stated Mechling, "and the bad news is the same thing, in that it is hard to do and the public has a limited attention span for these things." He challenged the conference audience to turn their ideas into actions that can sustain the support needed to meet our immediate and long-term homeland security requirements.

# CREATING AN INFRASTRUCTURE FOR HOMELAND SECURITY

## *Session 1-1: Evolving Towards a Culture of Cooperation*

### **Moderator:**

**Robert D. Atkinson**, Vice President, Progressive Policy Institute

### **Panelists:**

**Joyce Doria**, Senior Vice President, Organization and Management Team, Booz Allen Hamilton

**Peter Verga**, Special Assistant for Homeland Security, Office of the Undersecretary for Policy  
Department of Defense

**Melissa C. Wojciak**, Staff Director, House Subcommittee on Technology and Procurement Policy  
U.S. House of Representatives

Changes in the way government buys technology and manages its personnel were among the key priorities of speakers at this session on efforts to foster greater cooperation.

All agreed that the challenges of changing organizational culture and making effective use of technology remain daunting. “It took less time to build an atomic bomb than it did to build a student visa system,” said Robert Atkinson, Vice President of the Progressive Policy Institute and the session moderator.

**Policymakers must recognize the “tribal” nature of individuals specifically, their loyalty to an agency or organization that leads to battles over funding and turf.**

To promote efficiency, he said, the government must change its procurement practices to encourage timely, integrated technology purchases. Designating a chief information officer for homeland security can help embed technology into the process, he said.

Efficiency also requires centralized contracting authority and a single site to review homeland security needs, said Melissa Wojciak, Staff Director of the House Subcommittee on Technology and Procurement Policy, chaired by Representative Tom Davis (R-VA). “We have to purchase better and faster,” she said. “We’ve seen too much time go by without purchases in a timely manner.”

In legislation to create a Department of Homeland Security, House members want to create a framework that encourages business process planning and breaks down cultural barriers on the sharing of information, she said. Another goal is for increased sharing with the private sector, which manages key components of the nation’s infrastructure. “The only way to see that our infrastructure is protected is to partner with the private sector,” she said.

But the obstacles facing federal agencies are primarily bureaucratic, said Joyce Doria, Senior Vice President at Booz Allen Hamilton. An organizational psychologist, Doria said policymakers must recognize the “tribal” nature of individuals specifically, their loyalty to an agency or organization that leads to battles over funding and turf.

The best way to combat these influences is through top-down management and executives committed to sharing information. “Deal with conflict upfront,” she said. Doria also cautioned that while planning has its place, real-world implementation is paramount to avoid duplication and complexity. “Design is 10 percent, and implementation is 90 percent,” she said.



*Joyce Doria, Booz Allen Hamilton*

When reorganizing its homeland security responsibilities, the federal government also may benefit from lessons learned at the Department of Defense, which was created in 1947 as a merger of the nation's largest military services.

DoD "is an experiment that is not completed yet," said Peter Verga, Special Assistant for Homeland Security for the DoD's Under Secretary for Policy. However, he noted, the agency can offer valuable advice on how to set responsibilities among diverse players and merge different philosophies into specific objectives.

---

## *Session 1-2: Maximizing Resources for E-Government and Homeland Security Integration*

### **Moderator:**

**Shane Harris**, Assistant Technology Editor, Government Executive Magazine

### **Panelists:**

**Lt. Gen. Joseph K. Kellogg**, Director of Command, Control, Communications and Computer Systems, J-6, Joint Staff

**Joel Willemsen**, Managing Director, IT, U.S. Government Accounting Office

The federal government has 55 different databases that deal with security threats, and the challenge for E-Government advocates is to promote interoperability and continuity so that critical information gets to those who need it.

Representatives of civilian and military agencies cited these statistics and issues, which included frank discussion of the potential obstacles ahead. For example, 11 agencies will need to communicate closely if the government wants to stay current on information from these various databases, said Lt. Gen. Joseph K. Kellogg, Director of Command, Control, Communications and Computer Systems, J-6, Joint Staff. In some cases, he said, "the databases are not linked." But there is precedent that suggests the government can improve cooperation and information sharing, he added.

During the past decade, he said, agencies were able to integrate systems architecture to monitor worldwide anti-drug efforts. In Afghanistan now, the military works closely with the FBI and other agencies to arrest suspected terrorists.

Moreover, new technology allows for greater real-time sharing of information, said Kellogg, citing improvements since the Persian Gulf War in 1991. While Gulf War commanders had to travel near the battle sites, DoD leaders now "can manage the war field from Washington," he said.

But true cooperation will require a government-wide commitment to enterprise architecture and integrated systems, said Joel Willemsen, Managing Director, Information Technology, at the U.S. Government Accounting Office. Too many different systems make the homeland security operation "unfriendly to the end user," he said.

But led by the Office of Management and Budget, the Federal Government is moving forward on establishing standardized enterprise architectures. More progress is needed, he said, but there is "more of a push for it than at any time since we've been involved."

---

**Too many different systems make the homeland security operation "unfriendly to the end user."**

---

Perhaps the government's most daunting challenge is providing interoperability for the hundreds of systems used by bureaus that will become the new Department of Homeland Security. "We may have to think about junking 'as is' [systems] to get to something new," Willemssen said. The key issue, he added, is determining what information to get to decision makers as quickly as possible.

---

## *Session 1-3: Securing Public Health Services — A Cross-Jurisdictional Approach*

### **Moderator:**

**Ivan C.A. Walks, MD**, Ivan Walks and Associates

### **Panelists:**

**Georges Benjamin, MD**, Secretary of Health, State of Maryland

**Steve Charvat**, Director of Training, Exercise, Planning and Mitigation, D.C. Emergency Management Agency

**Dorothy Webman, MD**, President and Chief Executive Officer Webman Associates



*Dr. Ivan Walks, Moderator*

Outbreak tracking and management are essential in the post 9/11/01 world of public health, say experts who also plan greater reliance on new technologies.

The events of September 11, 2001, and the subsequent anthrax scare last October ushered in a "new world of public health" that requires faster response times and improved tracking and sharing of information, says Georges Benjamin, Secretary of Maryland's Department of Health and Mental Hygiene. "The science changed right in front of us."

---

### **"The science changed right in front of us."**

---

The old approach may have allowed researchers a few days to investigate and review data on smaller, self-contained outbreaks, such as food poisoning. But time is of the essence with potential threats such as smallpox, anthrax and plague, according to Benjamin, since a speedy diagnosis may cut potential casualties by as much as 90 percent.

Citing anthrax cases from the Brentwood Post Office in Washington, D.C., Benjamin said afflicted patients showed up at area hospitals in Maryland, Virginia and the District of Columbia. But it took time for regional health officials to recognize a troubling trend. As a result, health care facilities and departments need locally connected surveillance and data tracking systems.

Georges also cited five key ingredients in managing a potential health epidemic:

- Data generation
- Collection and analysis
- Outbreak tracking
- Outbreak management
- Recovery



Another requirement is technology that supports health care workers, including built-in redundancy to assure the flow of information in emergencies.

Experts from Washington, D.C., and New York City also described responses in their cities in the days after September 11, 2001. In the nation's capital, officials quickly realized their emergency plans needed improvements to deal with a new era of terrorism. New plans were in place within two weeks, said Steve Charvat, Director of Training, Exercise, Planning and Mitigation, D.C. Emergency Management Agency.

The city also reconstituted some of its working groups used for Y2K planning. With Y2K, "Nothing happened because we planned ahead," he said. One outgrowth of the new planning effort is a family preparedness guide for D.C. families that is available in seven languages.

In New York City, emergency workers were deluged with food and technology donations but sometimes could not capitalize on these contributions, said Dorothy Webman, President of Webman Associates. In Lower Manhattan, workers needed handheld devices instead of desktop computers, while food donations were made to the Red Cross even though that organization is not designed to accept food donations.

Elsewhere, poor families found that food stamp cards failed to work at some local stores, she said, while food donations—particularly from restaurants—usually did not reach isolated senior citizens.

As a result of her work, Webman listed core priorities for disaster planning, beginning with immediate disaster relief such as food, clothing, shelter and crisis health care. Other priorities include:

- Long-term mental health services
- Community mobilization efforts
- Public health services
- Housing assistance
- Business recruitment and development

Cities also need to train volunteers for emergency situations and link their legacy computer systems to other local information systems, Webman added.

---

## *Session 1-4: Translating Technologies to Capabilities*

### **Moderator:**

**John Sindelar**, Deputy Associate Administrator, Office of Governmentwide Policy  
General Services Administration

### **Panelists:**

**Gila J. Bronner**, President, Bronner Group

**Major Shawn Hollingsworth**, Assistant Deputy Director, Fort Gordon Battle Lab

**Mark Spooner**, Innovative Technology Division manager, ANSER

**Hal Wilson**, Lead Technology Officer, Defense Mission Systems Group, Northrop Grumman IT

Thinking out of the box and a willingness to evaluate a range of solutions were among the suggestions of panelists at this workshop that included private sector analysts, a military leader, and a consultant to local emergency management agencies.

"There are no silver bullet solutions," said Mark Spooner of ANSER, a non-profit public research

group that evaluates IT solutions. But decisionmakers can make the right decisions if they know their environment and understand their technology. Specifically, he urged homeland security professionals to:

- Evaluate yourselves and your opponents
- Define the role of subject matter experts in the management hierarchy
- Understand technology and the environment where it is used
- Clarify roles of team members, including roles of technical and operational staff

Hal Wilson, Lead Technology Officer at Northrop Grumman IT, said public sector leaders need to “get out of the box” when translating technologies into capabilities. Secure wireless and interoperability across multiple platforms must be major goals in this exercise. And while most activity must focus on the present, it’s important for decisionmakers to balance current needs with planning for the future.

---

**It’s important for decisionmakers to balance current needs with planning for the future.**

---

The 90 clients of the Bronner Group include several local agencies seeking to develop real-time intelligence sharing, protocols, and systems to deal with emergencies. Gila Bronner, the firm’s President, cited her work in the Chicago area to promote information-sharing and training for volunteers and staff.

As evidence of what she termed a “more holistic approach” to collaboration, one Illinois agency changed a key job title from Director of Emergency Communications to Director of Emergency Management.



*Major Shawn Hollingsworth, Fort Gordon Battle Lab*

---

## *Session 1-5: Information Assurance—Integration with Homeland Security Systems*

### **Moderator:**

**Larry Castro**, Homeland Security Support Coordinator, National Security Agency

### **Panelists:**

**Dave Carey**, Vice President, Information Assurance Center, Oracle Government Education and Health

**Dr. Jeffrey Hunker**, Dean, Heinz School of Public Policy and Management, Carnegie Mellon University.

**John McCumber**, Strategic Program Manager, Symantec Corporation



Federal and private sector decisionmakers face many challenges before information assurance gains full integration with homeland security systems. This point was a common refrain at the Homeland Security Conference that featured four speakers with a variety of ideas to enhance IA's visibility on the homeland security radar.

Public/private partnerships are vital to linking IA with homeland security, said Jeffrey Hunker, Dean of the School of Public Policy at Carnegie Mellon University. To forge partnerships, both sectors can fall back on the informal links created during Y2K planning. Development of a national information protection center also would help promote a partnership framework.

Dr. Hunker shared his concern that information assurance may not receive enough visibility in the new Department of Homeland Security. Under one proposal, IA would become part of the same office as information analysis. If approved, that approach would serve to "push down the importance of information assurance," he said.

According to Hunker, major obstacles to public/private partnerships include:

- Privacy concerns
- Ambiguity between U.S. national interests and the interests of multinational corps
- Legal and liability systems
- Information-sharing
- Human interface challenges
- Management practices and protocols to usher in new generations of technology

Within the federal government, issues of culture, cost, and access are among the paramount concerns when discussing information assurance, other presenters said.

"We have lots of data all over the place," said Dave Carey, Vice President, Information Assurance Center, for Oracle Government, Education and Health. The problem, too often, is that decisionmakers "can't see the whole picture."

He recommended that the federal government not build a single information system for homeland security but instead adopt a loosely integrated system in which agencies commit to specific standards on issues such as integrity and security.

Independent evaluation also is essential to ensure that government purchases quality off-the-shelf products with minimal customization, thereby cutting down on costs, he said.

Both the government and private sector must increase their cybersecurity investments to meet IA needs, said John McCumber, Strategic Program Manager for Symantec Corporation. For business, one solution may be accelerated depreciation for IT purchases. A shortage of IT security professionals is another challenge that demands public and private sector attention, he added.

In the federal sector, agencies also can save costs by working with companies that have a range of security products. Using multiple solutions from various vendors can affect cost and compatibility, remarked Mr. McCumber.

**Within the federal government, issues of culture, cost, and access are among the paramount concerns when discussing information assurance.**

# BUILDING INTEGRATED HOMELAND SECURITY OPERATIONS

## *Session 2-1: Organizational Constructs that Work*

### **Moderator:**

**Stephen M. Ryan**, Partner, Manatt, Phelps & Phillips

### **Panelists:**

**Nancy Wong**, Deputy Director, National Outreach and Awareness, U.S. Critical Infrastructure Assurance Office Department of Commerce

**Tony Frater**, G2G Portfolio Manager, Office of Management and Budget

**LTC Mike McNamara**, Professor of Systems Management National Defense University

**Richard Morris**, Advisor to the Director, Office of Public Health Preparedness Department of Health and Human Services

This session explored the roles, responsibilities, and authority of government organizations as national policies are developed to deploy a Homeland Security strategy. In addition, the panel sought to identify the technology and security expertise offered by the core constituent organizations. Panelists indicated that partnerships, cross-agency initiatives, education, and implementation processes for IT solutions are important elements in fostering successful Homeland Security initiatives.

In the Critical Infrastructure Assurance Office (CIAO) at the U.S. Department of Commerce, efforts began in 1988 to help develop partnerships with private industry that support protecting the national IT infrastructure, with recent outreach activities focused on cybersecurity. Ms. Nancy Wong remarked that the word “partnership” is overused, and that principles of building strategic alliances need to be enacted to make partnerships more meaningful.

In the private sector, Ms. Wong stated, form (structure) follows function, but in the public sector, the reverse is too often the case. Organizational structure should not dictate business functions or processes, but should flow from them. In many respects, government is intended to move slowly because this approach fosters stability. In today’s environment, there is a need for change. Ms. Wong highlighted the need to evolve government structures in a more fluid way.

In response to Presidential directives, the Office of Management and Budget has been expanding its E-Government activities that are instrumental to supporting homeland security efforts. OMB’s Tony Frater mentioned three important projects:

- (1) Project SAFECOMM for wireless interoperability, which involves a number of large organizations, including the DoD and FEMA.
- (2) Geospatial OneStop, which may become a backbone of homeland security as considerable funds are being spent on geospatial information, and the federal investment should be aligned with state and local government authorities who, by necessity, collect and maintain higher resolution data.
- (3) A disaster management portal to streamline emergency communications and response.

**In many respects, government is intended to move slowly because this approach fosters stability. In today’s environment, there is a need for change.**



*Stephen Ryan, Tony Frater, Mike McNamara, Nancy Wong, and Richard Morris.*

Since many agencies cooperate on these projects, there are cultural issues to be resolved. Among the barriers to change are determining ownership of processes and customers, and the lack of a federal enterprise architecture to help bring together disparate systems. OMB will give priority to cross-agency initiatives that resolve these cultural gaps and include genuine partnerships with state and local governments.

NDU's Information Resources Management College was tasked with building a homeland security course that would be an elective under its E-Government curriculum. NDU's Colonel McNamara noted that

domestic terrorism is not new, but has clearly increased in the recent past, requiring all government organizations to take protective measures. PDD 39 signed in June 1995 specified responsibilities for federal agencies in combating terrorism, and in May 1998, PDD 62 provided more information on the responsibilities of specific agencies.

Colonel McNamara pointed out that resiliency has received increased attention as a business requirement for government operations. Most businesses that had crisis management or business continuity plans that had not been rehearsed found that in an actual crisis, the plans had deficiencies. Organizations that rehearsed planned scenarios were better able to respond to actual events. Tabletop exercises provide a relatively inexpensive way to test such plans, but have limited value, whereas field exercises provide a better simulation, but are expensive and time-consuming.

The newly-established Office of Public Health Preparedness at the Department of Health and Human Services will assist state and local governments to improve their public health systems with increased preparedness planning and readiness assessment. An important shift for HHS will be to move its focus to address situations outside of hospitals and doctors' offices, a change that requires new enabling technologies, including two-way communications and the ability to accommodate heterogeneity among information systems. Mr. Morris said that HHS hopes to make use of supply chain management capabilities and other technologies used in the private sector and that of \$1.1 billion in funding, 25% will be directed to information technology.

---

## *Session 2-2: Securing the Transportation Infrastructure*

### **Moderator:**

**Rebecca L. West**, Deputy Chief of Staff, Office of Information and Security Technologies  
Transportation Security Administration

### **Panelists:**

**Phillip Loranger**, Chief of Enabling Access Technology Team, Federal Aviation Administration

**David Price**, Special Assistant for the Executive Director, Office of Administration  
Federal Highway Administration

**Susan Knisely**, Advisor to the Deputy Administrator, Federal Transit Administration

All transportation modes are under review with an eye toward improving public safety. On the highways, as in the public transit and air traffic systems, the challenge comes down to balancing freedom of movement with security in the large, complex, and heavily-used national transportation systems.

Ms. Rebecca West of the Transportation Security Administration listed President Bush's three initiatives relative to terrorism: winning the war, protecting the homeland, and maintaining the strength of the national economy. The objective is to ensure freedom of movement, people, and commerce. To achieve this goal, new processes for screening passengers, baggage, cargo, and otherwise securing commercial airports have begun. The TSA is working with a range of organizations to implement new access controls and secure communications.

The magnitude of the system, said Mr. David Price of the FHWA, presents significant challenges with respect to protection. The highway system includes 4 million miles of roads, 575,000 bridges, and 400 tunnels that together handle 5 trillion passenger miles and 4 trillion freight miles of traffic. The highways account for 72% of all domestic shipment, with bridges and tunnels as the most vulnerable part of the system.

Mr. Price identified a number of actions the federal government can take to support state and local efforts to protect highways. It can serve as a communications hub and develop partnerships, collect and distribute best practices information, and support training. The federal government also can provide research and development funding, threat information, emergency response, and even military deployment if needed.

**The objective is to ensure freedom of movement, people, and commerce.**

FHWA currently supports a number of efforts to improve national roadway security, including the American Association of State Highway and Transportation Security's Task Force on Transportation Security and the recently completed Highway Vulnerability Assessment Guide, including identification of critical information, threats, and countermeasures.

Ms. Susan Knisely outlined the present activities of the Federal Transit Authority in supporting a transportation industry that employs 400,000 employees and has an infrastructure valued at \$1 trillion. FTA provides \$7.2 billion per year in capital grants to transit agencies, along with training, technical assistance, and a limited amount of research. Concern about terrorism directed at the transportation industry centers around the potential for mass casualties, attacks on high visibility landmarks and national icons, and the potential economic impact.

Like the highway system, the transit system is open and accessible by design, with access points that are often unmonitored. Security equipment is limited, and awareness of security issues varies among employees. In general, security measures are isolated rather than systemic.

Keeping American communities safe, Ms. Knisely noted, requires balancing three factors: mobility, economic viability, and security. As of 9/11/01, emergency response plans were in place, agencies had conducted drills, and first responders had established trusted relationships. All of these elements combined to help produce a functional response team despite the chaotic environment. FTA is developing best practices and guidelines that include procedures for managing chemical and biological incidents and decontamination procedures.

On the morning of 9/11/01, Mr. Phillip Loranger's greatest fear was that the aircraft attacks would be followed by a cyberterror attack. The FAA was faced with landing more than 5,000 aircraft safely, which was done in ninety minutes; fortunately, the FAA's critical systems remained operational. Since then, the

agency has begun developing a strategy to establish universal, positive verification for all FAA personnel and operational entities. Mr. Loranger identified cyber-protection as the key to countering “weapons of mass disruption.”

The FAA’s Access Enabling Technology Team was established in December 2001 to work toward enterprise-wide security in the areas of positive verification and control, authentication, and other aspects of security. Mr. Loranger summarized the FAA’s approach as leveraging COTS to acquire and integrate access technologies, organizing multiple security initiatives, developing a plan to provide an enterprise-wide solution, and partnering with FAA entities and private industry to improve access security across all operations.

---

## *Session 2-3: Technology at the Border*

### **Moderator:**

**Jim Litchko**, President, Litchko & Associates

### **Panelists:**

**Chuck Archer**, Vice President, Homeland Security  
Northrop Grumman IT

**Dr. Ned Futoran**, Program Manager  
Federal Law Enforcement Training Center  
Department of the Treasury

**Scott Hastings**, Chief Information Officer  
Immigration and Naturalization Service



This panel discussed the programs and technological options under consideration for improving border security. Panelists recalled the difficulties they experienced in law enforcement when they were unable to access information they needed, and focused attention on the importance of clearly stating business missions prior to implementing technology. A commitment to training also was cited as an essential element of effective border protection.

Mr. Archer noted the severe testing that domestic reactive systems underwent after 9/11/01, and called for government and industry to combine to stop terrorists at the border. A first priority should be training and providing access to critical data. As a young FBI agent, Mr. Archer experienced frustration when he could not access other agencies’ databases. While information sharing has improved in recent years, there is room for improvement.

The capabilities of government databases also have improved, with the IAFIS fingerprint system now confirming matches in two hours when the fingerprint is submitted electronically, rather than requiring a month. The FBI’s database contains 35 million fingerprints, and 65,000 per day are submitted for analysis.

Biometrics offers a more reliable way of positively identifying individuals at the border than do current controls, Mr. Archer said. This is a particularly useful approach when people are attempting to enter the United States under multiple identities.



Having a secure border after years of openness is a big adjustment, noted Mr. Scott Hastings, CIO for the INS. More than 500 million people annually enter the U.S., which puts the \$6 billion operating budget for INS in some perspective.

New technology cannot be effectively defined until the business missions are clearly stated. One of the challenges faced by INS is deciding what information technology should be retained and what should be scrapped. Before defining new requirements, INS should integrate and stabilize what they have. Better use of existing equipment will require conducting an inventory and analysis to see what is available, what is redundant.

**Having a secure border  
after years of openness is  
a big adjustment.**

The Federal Law Enforcement Training Center trains all law enforcement personnel except those from the FBI and DEA. Dr. Ned Futoran of FLETC reiterated the concept that the homeland is secure when hometowns are secure, which requires that training be directed toward the “first warrior” or first responder. Drawing an analogy to computer maintenance, he pointed out that most organizations pay about 15% of the capital value for maintenance of computers, and suggested that we invest a comparable percent on maintaining human capital through training.

Dr. Futoran believes that neither technology nor extra funding is the answer, but rather, focused training that answers four questions: (1) What do we need to know? (2) Who needs to know it? (3) When do they need to know it? and (4) How much do they need to know? The borders today are porous and quick solutions are sought. A range of training options are available, from online courses to simulations. Training effectiveness should be measured, so that lessons learned can flow into the next training deployment.

---

## *Session 2-4: Technology Priorities for State and Local Governments*

### **Moderator:**

**Donald V. Evans**, President, Strategic Business Products Corporation

### **Panelists:**

**Linda Burek**, Chief Information Officer, State of Maryland

**Matt Lampe**, Director, Strategic Planning, Department of Information Technology  
City of Seattle, Washington

**David Sullivan**, CIO, City of Virginia Beach, VA, and Vice President of Metropolitan Information Exchange (MIX)

State and local governments bear significant responsibility for ensuring homeland security. Since implementation of security sometimes can make business systems more difficult to use, it is important to encourage buy-in from all stakeholders in advance. Simplifying the infrastructure is one way to ensure more local government collaboration, as well as establishing cross-agency approaches for emergency management, enterprise security, and communications standards.



*Linda Burek, David Sullivan, and Matt Lampe.*

Mr. Donald Evans, the moderator, provided some statistics to illustrate the extent of the needs at the state and local level: 50 states, 5 territories, 19,200 municipalities, 16,000 townships, 15,000 school districts, 512 Native American Nations. In Virginia alone, we have 130 counties and cities. However, 80% of the population lives in just 10 of them. This allows us to focus on areas of greatest need.

Panelists began by identifying what they believe to be the most important issue facing their organization. Ms. Linda Burek from the State of Maryland stressed that although state and local governments have emergency plans in place, they need to be tested to ensure their viability, with a focus on eliminating weak links.

According to the City of Seattle's Mr. Matt Lampe, implementing some technology policy can impede business processes. As security becomes increasingly important throughout government operations, systems can become more inconvenient for users. He said the best way to govern security is not at the technical level, but at the business level. Decision-makers need to get involved in IT security operations and include others, such as legal and risk management staff, so that everyone supports the plan from the outset.

Mr. David Sullivan said his greatest concern was regional cooperation. His city, Virginia Beach, VA, is one of seven in the Hampton Roads area, which contains 400,000 people in a 310 square mile area. Hampton Roads has been working on regional cooperation for some time, and has established a criminal justice system for all 11 jurisdictions. Connected to different offices by a T-1 line, the regional database on criminal activity is more in-depth than those available from state or federal databases. Mr. Sullivan concurred that technology is not the most difficult issue; people are. The criminal justice database in use in his region took 10 years to implement.

Given that the most likely vulnerability to cyberterror is local, the question was raised by a participant as to whether the federal government could develop tool sets, or whether the state and local governments have to develop everything from scratch. Ms. Burek pointed out that the federal government cannot get too far ahead, or it will lose sight of the local government requirements. However, Mr. Lampe said that in some cases the federal government could be of great help. He sees few computer-based emergency management systems at the local level and suggested that perhaps FEMA could develop one that ties into GIS information, with the potential for adding a local extension.

One policy that could be put into place at the state level to help local jurisdictions is simplification of the infrastructure, Mr. Sullivan remarked. In the Hampton Roads area, they have a centralized IT system for 25 lines of business. However, the police department needs to interact with many states, all of which have different standards. Ms. Burek mentioned that the General Assembly of Maryland is considering a bill to support discussion of standards with support from the Lt. Governor's office.

The best way to maintain state and local interest in homeland security under current economic limitations, according to Mr. Lampe, is for the federal government to fund key initiatives rather than just distributing money. For example, they should seek out government solutions applications that look at security, and support them.

---

**Emergency plans need to be tested to ensure their viability, with a focus on eliminating weak links.**

---



## Session 2-5: Industry Preview — What's Over the Horizon

### Moderator:

**Jim Kane**, President, FSI (Formerly Federal Sources, Inc.)

### Panelists:

**Mark Gerencser**, Vice President of Global Strategic Security, Booz Allen Hamilton

**Mike Grady**, Chief Technology Officer, Northrop Grumman IT

**Tim Hoechst**, Senior Vice President, Technology, Oracle Government, Education, and Health

**David Roberts**, Co-founder, ZAPLET

This panel discussed the technologies that are being developed to support an integrated homeland security infrastructure. As new technologies provide more capabilities, they also complicate enterprise security efforts. Software is being developed that evaluates input from multiple security systems to determine actual risk and provide a response. Across all the emerging technologies, acquisition processes are problematic because of the long cycle times. Homeland security gaming exercises between business and government have been useful in determining communications problems and ways of overcoming them.

Keeping systems secure is not just a technical problem but a combination of people, process, and technology, Mr. Mike Grady said. Maintaining security is becoming more difficult as new activities, such as Web services and J2EE, are being launched. Wireless technology also complicates security, as do self-organizing networks. Today's systems have many security inputs, such as virus checkers, firewalls, PKI, and intrusion detection systems.

Biometrics also is an emerging technology, and we need to balance errors of omission and commission, said Mr. Grady. The system should not block someone who is authorized to have access. Many people also want non-invasive methods that do not require, for example, scanning of the eyeball by a laser.

Information is the most powerful self-defense weapon we have, said Oracle's Mr. Tim Hoechst. We need to find ways to establish relationships between federal, state, and local entities. People are possessive of their data, though the barriers are starting to break down and it is important to continue this trend.

Standards for secure sharing of information at rest and in motion must be established. However, security entails technical and social issues and some laws must be revised so that information becomes more useable.

ZAPLET's Mr. David Roberts continued the theme of social barriers, adding that even when social barriers come down, technical ones remain. He identified four challenges that need to be overcome before intelligence can be fused:

- (1) **Collaboration tools are limited.** E-mail as a collaboration tool is effective for one-to-one contact or for one-to-many, but for many-to-one it is not. When a recipient is swamped with messages, sorting them out is time-consuming.
- (2) **Application development is time-consuming.** New ways of developing applications in a more pre-assembled way will allow use of staff with less expertise.



*Jim Kane, David Roberts, Mark Gerencser, Tim Hoechst, and David Roberts.*

- (3) **Lack of end-to-end processes.** Few solutions are available where government organizations have fused an end-to-end process. Usually, an e-mail, phone call, or meeting is required to complete a process.
- (4) **Slow rate of technology adoption.** The acquisition process takes one to two years, whereas the half-life for software is six to nine months.

Mr. Mark Gerencser of Booz Allen Hamilton believes that new constructs for public-private partnerships are needed. During the Cold War, the government could deal with the military threat, but in reality the United States won the Cold War economically, not militarily. The targets now are new—the things industry owns are targets, so we need new ways to protect them. Industry has a new social responsibility; the government can no longer say it's "Business as usual."

As an example, Mr. Gerencser discussed recently conducted war games focused on bioterrorism issues with CEOs from healthcare companies. It was interesting to see, Mr. Gerencser reported, how government and industry interacted—the barriers were obvious and the assumed responsibilities were different. Participants included HHS, Blue Cross/Blue Shield, Kaiser, and the CDC. The first outcome was poor. New partnerships are required because neither industry nor government can solve the problems alone. Leadership from all sides and a collaborative style were proven to be key ingredients.



---

**New partnerships are required because neither industry nor government can solve the problems alone.**

---

Some of the ensuing discussion centered around the need for checks and balances and accountability. One audience member asked for guidance about whom the citizens should trust, and another added that in many of the plans, direct input from consumers (such as passengers or patients) seems to be missing.

With respect to partnerships, a panelist agreed that industry and government should develop partnerships but should remember that the two have different strengths. Business is more efficient, he said, but government is good at protection. Another panelist noted that we are not as good at partnering when we are not in crisis.

One panelist said that we need to share conclusions rather than raw data—not everyone needs source data. Even if agencies shared this data, it might not be used because they need a context for the data.

Another took the position that Homeland Security is a complex issue, and that it is wrong to think there is a simple answer. He believes the United States wants an environment of trust and freedom, not an authoritarian regime. It is important, he said, to look at causes as well as symptoms.

The moderator concluded the session by asking each panelist what would be the leading issues three years from now. Two panelists said privacy, one said the same issues as now (no change), and another said human rights.

### *Plenary Session 2: Attendee Discussion Forum: Technologies and Strategies for HLS — Today and Tomorrow*

#### **Moderator:**

**Michael J. Mestrovich, Ph.D.**, President and CEO, Unlimited New Dimensions, and HLS 2002 Program Chairman

#### **Panelists:**

**Gila J. Bronner**, President, Bronner Group

**Larry Castro**, Homeland Security Support Coordinator, National Security Agency

**BG U.S. Army Jack Pellicci (Ret.)**, Group Vice President, Business Development, Oracle Government, Education, and Health

**David Tubbs**, Former Executive Director, Utah Public Safety Command and Director of Security, 2002 Winter Olympics

Information sharing, business continuity, and cross-agency collaboration were three of the key issues identified by moderator Michael Mestrovich as the Homeland Security 2002 Conference drew to a close. There was a strong consensus about the need to train people to overcome cultural issues and turf battles, but participants recognized that so far, only a few examples of success have emerged.

Going back to basics, a panel member noted “government” means “to steer,” but that the government now may be doing more rowing than steering. One of the appropriate roles for government identified by audience members is that of developing reusable methods and systems. In this respect, establishing a federal enterprise architecture framework (“FEAF”) was viewed as a timely and effective use of government resources. When the issue was raised about the experience of the Department of Defense with interoperability might prove useful in civilian settings, Dr. Mestrovich said he had not observed significant acceptance of these standards outside the military environment. Information security, another key concern, should be included in system design, rather than added afterward, and must be balanced by respect for privacy.

**“Everybody wants to transform, but nobody wants to change.”**

NSA’s Larry Castro observed there had been some heartening progress over the past six months. At the last E-Gov Homeland Security Workshop held in December 2001, participants supported the concept of an Office of Homeland Security at the cabinet level. This hope has been realized, which will provide an organizational framework for Homeland Security efforts. As the Congress prepares to create a new Department of Homeland Security, other cabinet agencies are moving ahead with their own HLS plans. The CIA has appointed Winston Wiley to the new post of Associate Director for Homeland Security, while the Pentagon also will fill a new senior HLS post.

In addition, Mr. Castro cited the promise of the rollout of a National Strategy for Homeland Security, which occurred six weeks after the December 2001 Workshop. A National Advisory System has been developed for classifying sensitive homeland security information to be provided at the state level. Mr. Castro sees the need for the federal government to better coordinate research and development programs with technology investment, and for the establishment of a common intelligence platform.

Although innovative solutions are more likely at the local level where there is less bureaucracy,

Ms. Gila Bronner reminded participants that because of the economic downturn, state budgets are lower, a reality that is affecting local governments across the board. For example, in Chicago, Emergency Services was renamed Emergency Management and given a broader charter, but its budget remains the same.

On the federal level, such innovations may take time due to issues centered around protection of turf, funding and differing agency cultures. “Everybody wants to transform, but nobody wants to change,” said BG U.S. Army Jack Pellicci (Ret.), Group Vice President, Business Development, Oracle Government, Education and Health.

Considerable concern arose around the issue of funding. Ms. Bronner said that she was not seeing many dollars reach the state and local level; Mr. Pellicci added that block grants are available, but there is a qualification process and most of the initial money has been allocated. The large number of recipients would seem to indicate that each grant is for only a modest amount. Mr. Castro estimated that a third of the required money for homeland security will come from the federal government and a third from the states, but said the balance must come from the private sector. Industry needs to take responsibility for funding its own IT projects to increase security.

Homeland security is in some respects a grassroots movement, said David Tubbs, that is determined by individuals who have been appointed to head this function in the states. However, in other respects it represents a federal movement, with directives coming from organizations such as Transportation Security Administration. Some of the requirements are coming up from the states, such as Florida’s risk assessment that specified needs for education and training. These, in turn, disseminate through the agencies. Thus, a two-way flow of information is beginning to occur.

One project that already had been launched prior to 9/11/01 is a First Responders collaborative visualization project in New York City, a \$50 million effort to provide spatial data and imagery. Often, these kind of local datasets are more detailed and more accurate than those available from national sources. Establishing such visualization capabilities will benefit organizations across government.

Forum moderator Michael Mestrovich, President of Unlimited New Dimensions, launched into the ID discussion by seeking a show of hands among attendees who supported some form of national identification card. At the last E-Gov Homeland Security Workshop held in December, three-fourths of the crowd opposed the idea, he said. At this forum six months later, about two-thirds of the audience supported the concept.

Most forum speakers also supported the identification card, particularly if it would not undermine the principles of basic civil rights. But several audience members criticized the idea, stating it could hurt legal immigrants, those with limited English skills, and individuals who move frequently. The system also could be vulnerable to fraud. Tubbs noted that even an ID card would not solve all homeland security concerns. Issues such as border security and immigration rules also need attention, he said.

An important question is how state and local governments will know what they are supposed to comply with, when objectives have not been stated in a consistent way. Given that resources are limited, participants expressed a need for guidance in prioritizing homeland security objectives. The conference attendees agreed on the need for a continued dialogue about reaching desired standards for national homeland security, maintaining privacy while protecting Americans, and distinguishing efforts that sound good on paper from those that will be truly effective.



*Jack Pellicci, Larry Castro, Gila Bronner, David Tubbs, and Michael Mestrovich.*



## *Summary of Attendee Recommendations and Questions*

Conference attendees were invited to submit comments and recommendations to contribute to this Executive Summary Report. The following is a compilation of the submissions received.

### **Future Plans for Homeland Defense**

- What are the homeland defense plans for two, five and ten years hence? Are we taking the steps to have:
  - National biometric ID cards
  - A national citizen database
  - 100% inspection of inbound cargo
  - A smart visa and a tracking system
  - A sufficiently funded and robust intelligence activity to identify and track potential terrorists
  - A proactive effort to win over the hearts and minds of those who now hate the US and fan the terrorist flame
- How do we keep the American people from becoming complacent on the issue of homeland security without sensationalizing the issue?
- We have heard a lot about great plans and programs for various homeland security initiatives. When can we expect to see some measurements of success? Per Rudy Giuliani's comments earlier today, "That what gets measured gets managed."
- Remember when we built systems without architectures and it took an act of Congress to fix that? Every homeland security program mentions risk management but it does not seem feasible to build "well-architected IT solutions" without a holistic blueprint.
- Infrastructure security means more than protecting the national air transportation system and information technology. We have tremendous vulnerabilities in our water, electrical, and mechanical systems. I would like to see what coordinated efforts are ongoing to address these potential target areas.

### **Deploying Best Practices Across Government**

- The Department of Defense is required to operationally test, look at interoperability and information assurance before we 844 (take steps to procure) a process or system. Why does the federal government not have the same requirement?

- At the 2002 Winter Olympics in Salt Lake City, what was the secondary means of identification for police and other law enforcement officials after wearing colored jackets? If it worked well there, why not implement elsewhere?
- What, if any, value can the interoperability lessons learned by the DoD over the last 50 years of coordinated multi-service and multi-national responses to hostile actions against U.S. national interests provide to domestic and other international homeland security programs?
- We continue to have too much focus on computer systems and need for people to share information. Significant attention should be paid to analyzing specific case studies of how problems are being addressed today. The strongest speakers (mostly from government in this conference) consistently formulate their remarks around this kind of situational analysis. It was also very useful to hear the perspective of the private sector—what are the specific challenges to delivering homeland security solutions to disjointed government sectors. One panelist at the local level suggested that the "system" needs to be "less complex, not simple, but less complex". Another panelist suggested that the government needs to be able to operate better in non-crisis mode.



### **Introducing Innovations for Homeland Security**

- Is there or will there be a central contact for the Office for Homeland Security for the purpose of introducing projects and services essential to Homeland Security?
- What is the status of the trusted traveler card system? Will this new program be implemented by the Transportation Security Administration and on what timeline?

- You need to have more debates/discussion as opposed to panel—not enough time for Q&A, discussion, debate.
- War Time ID Cards—This approach acknowledges the special state we've been thrust into, warranting special kinds of identification, e.g. at airports.
- Common themes are the challenges of cultural change and interoperability. What would government agencies like to see from industry counterparts to assist them in working together more effectively?
- Industry representatives must emphasize homeland security solutions that are explained in the agency business context, not just demonstrations of new technology. Prime contractors can be particularly effective if they bring together their partners in a collaborative environment in which all players are visible, vocal and provide input to meeting agency requirements.

### Future Events

- We need to continue to have more discussion about the cultural and “people-oriented” issues as they relate to how federal, state, and local governments and organizations can most effectively implement homeland security programs.
- My suggestion for a future conference is to create tracks for defense trends and challenges; administrative trends and challenges; and health trends and challenges. We need to move beyond Information Technology and cover the specifics of these thematic areas in more depth.
- I would like to see more sessions on policy formation and implementation of operational issues, as well as discussion of the physical security considerations in many of these programs.

---

## HOMELAND SECURITY 2002 CONFERENCE PROGRAM ADVISORY BOARD

### CHAIRMAN:

**Michael J. Mestrovich, Ph.D.**, President and CEO  
Unlimited New Dimensions and Homeland Security  
2002 Program Chairman

### ADVISORY BOARD MEMBERS:

**Jeff Bolletino**, Vice President  
Electronic Government, Booz Allen Hamilton  
**Larry Castro**, Homeland Security Support Coordinator  
National Security Agency  
**Steve Cooper**, Chief Information Officer  
Office of Homeland Security  
**Donald V. Evans**, President  
Strategic Business Products Corporation  
**Jim Flyzick**, Special Advisor to Governor Ridge  
Office of Homeland Security  
**David L. Jerome**, Principal, Booz Allen Hamilton  
**Gary Lyles**, Executive Director, Strategic Planning  
Communication and Infrastructure Systems  
Northrop Grumman IT  
**Jerry Mechling, Ph.D.**, Director, Strategic Computing  
and Telecommunications in the Public Sector  
John F. Kennedy School, Harvard University

**Ron Miller**, Chief Information Officer  
Federal Emergency Management Agency  
**Jack Pellicci**, Group Vice President  
Business Development  
Oracle Government Education and Health  
**Mary Schiavio**, Partner  
Baum, Hedlund, Aristei, Guilford and Schiavo  
**Kent Schneider**, Vice President for Defense Infrastructure  
Northrop Grumman IT  
**Ivan Walks, M.D.**, Former Director  
DC Department of Health  
**Rebecca L. West**, Deputy Chief of Staff  
Office of Information and Security Technologies,  
Transportation Safety  
Administration



*Dr. Michael J. Mestrovich,  
Homeland Security 2002  
Program Chairman*



## Homeland Security: The Way Ahead

Homeland security—your organization has an important role to play in assuring homeland security. Booz Allen Hamilton has the capabilities and experience to help you protect your organization and fulfill your mission and business goals.

The President outlined several critical areas we all must address—we must be able to detect, prepare, and protect, and, as necessary, respond to and recovery from a terrorist incident. To achieve an acceptable level of security, all these critical areas must be woven into the security fabric of every organization's internal and external strategy.

From a national perspective, a number of major priorities have been identified. First ... police, firemen, medical technicians, and other “first responders” need readiness plans, new equipment, bioterrorism training and an effective alert system. Second ... researchers, hospitals and healthcare systems need extra support to combat bioterrorism. Third ... border control systems and processes are needed that identify and stop terrorists without slowing the flow of people and commerce. Fourth ... we must develop more efficient tools for information sharing, threat assessment and cyberspace protection. Finally ... other priorities include protecting the critical infrastructure, strengthening aviation security, assuring continuity of government, and supporting intelligence and defense activities that safeguard domestic security.

### Booz Allen Can Help

Booz Allen continues to help dozens of organizations with services supporting the full spectrum of homeland security—from first responder training to Bioterrorism preparedness, from continuity of government and continuity of business operations, Force Protection and counterterrorism planning and threat and vulnerability analysis and assessments, to strategic simulations and war games. Our depth and breadth of knowledge come from decades serving both government organizations and the world's leading corporations.

#### Booz Allen Homeland Security Capabilities

- |  |   |
|--|---|
| • Strategic Planning   | • Emergency Preparedness  |
| • Change Management and Organizational Reinvention                           | • Counter-terrorism and Anti-terrorism support                                |
| • Post Merger Integration  | • WMD Preparedness and Response   |
| • Wargames and Simulation  | • Continuity of Operations (COOP) and Continuity of Government (COG) Programs |
| • Workshops, Seminars, and other Analytical Support                          | • First Responder Training  |
| • Information Sharing and Interagency Collaboration                          | • CBRNE Preparedness  |
| • Infrastructure Assurance (IA) and Critical Infrastructure Protection (CIP) | • IT Solutions  |
| • Information Operations (IO)  | • Business Resilience (Private Industry)                                      |
| • Force Protection / Physical Security                                       |   |

Booz Allen's unique blend of government and private industry expertise enables us to understand homeland security issues at all levels of government—federal, state, and local—and enables us to help private enterprises integrate all dimensions of security in support of overall business strategy.

We can help you understand your security needs and develop an action plan to coordinate your essential “next steps.” We'll work with you to define and prioritize your security requirements ... determine your roles and responsibilities ... rally senior executives ... coordinate security requirements with other organizations ... monitor results ... strengthen capabilities ... and build partnerships with thought leaders to stay ahead of the homeland security issues and, more broadly, the larger, strategic security curve.

### About Booz Allen

Booz Allen is a privately owned, international management and technology consulting firm which serves business and government clients worldwide. We have over 10,000 employees and have worked for all of the major agencies of the U.S. federal government, the U.S. Congress, most of the U.S. Fortune 500 companies, and the largest industrial and services corporations around the world. We have offices on six continents and have served governments and industries in more than 75 nations.

Booz Allen Hamilton combines strategy with technology and insight with action working with clients to deliver results today that endure tomorrow.

For more information, please contact us at [HomelandSecurity@bah.com](mailto:HomelandSecurity@bah.com).



For the past 25 years, Oracle Corporation has been committed to the issue of Security. Oracle's Chairman & CEO, Larry Ellison, personally founded Oracle Corporation on a project within the federal Intelligence community. The clarifying events of September 11, 2001 have brought the need for safeguarding information even more sharply into focus. Oracle is ready to help you prepare for any potential threats with specific solutions tailored to the unique needs of the public sector - and always has been. Oracle Homeland Security covers three key areas:

#### **Information Assurance**

Safeguard against unauthorized disclosure of information by protecting your information systems. Built on the leading secure information management architecture available, Oracle solutions ensure that information is available only to those authorized to access it. Oracle technology helps maintain your information's availability, integrity, authentication, confidentiality and non-repudiation.

#### **Business Continuity**

Prevent destruction, corruption or degradation of information while protecting against a disruption of service. Oracle has long offered solutions for redundant systems to ensure that you are fully prepared to detect, prevent and respond to unforeseen disruptions in system availability, whether the result of natural disasters, internal sabotage or terrorist threats and attacks. These include redundant hardware and software, synchronous and asynchronous off-site backup, and online systems maintenance.

#### **Collaboration & Communication**

Oracle provides connected and disconnected wireless access, decision support and interaction centers to help you coordinate, collaborate and communicate across government agencies and with your constituents. Oracle provides a robust, integrated set of collaboration solutions for data warehousing and decision support, online information exchange, web portals and middleware.

*For Oracle's product solutions, online presentations, demos, and datasheets visit the Oracle Homeland Security website at [www.oracle.com/start](http://www.oracle.com/start), keyword: homeland*

# HOMELAND SECURITY

Collaboration within and beyond the organization has become critical to the defense of our homeland. Zaplet Appmail empowers secure collaboration across boundaries, removing barriers to information sharing and human interaction around critical knowledge.

## Zaplet™

### San Francisco Office

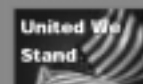
3000 Bridge Parkway  
Redwood Shores, CA  
94065

[www.zaplet.com](http://www.zaplet.com)

### Washington, D.C. Office

Towers Crescent Center  
8000 Towers Crescent Drive  
Suite 1321  
Vienna, VA 22182

FOR MORE INFORMATION ON HOW ZAPLET APPMAIL SYSTEM CAN HELP YOUR BUSINESS, CALL OUR SALES TEAM AT 1-800-823-7773, EMAIL US AT [APPMAIL@ZAPLET.COM](mailto:APPMAIL@ZAPLET.COM) OR VISIT OUR WEB SITE AT [WWW.ZAPLET.COM](http://WWW.ZAPLET.COM).



© 2001-2002, Zaplet, Inc. All rights reserved. Patents Pending. Zaplet, the Zaplet logo, and all other Zaplet-based marks are trademarks of Zaplet, Inc. All other trademarks and registered trademarks are the property of their respective holders.

Rapid distribution of information to participants across the firewall and into their email box

Access via multiple email clients (Outlook, Netscape Mail, Lotus Notes, etc.)



*Appmail reaches people in their inbox*



*Open to secure server application after authentication*

## SECURE COLLABORATION AND DECISION MAKING

- Reach everyone across organizations by delivering actionable information where people work—in their email inbox
- Collaborate safely with highly secure applications that reside on a central server, with features such as authentication, non-forwarding and self destruction
- Coordination around dynamic events. All information is current when read—not when sent



## E-Gov 2002

# Homeland Security Pavilion Exhibitors

ActionBase	e-InfoData.com	Netbotz
ANSER	Egoware	Northrop Grumman IT
Apex Innovations	EMC	SafeNet
Aspect Government Solutions	ForeScout Technologies	SAIC
The CENTECH Group	High Tower Software	SonicWALL
ChoicePoint	IES Interactive Training	Stratus
Data Management Group	Loudcloud	Symantec
Datastrip	MetaEdge	ValiCert
DigitalOwl	n-Link	Zaplet

## Featured Exhibitor



Symantec, a world leader in Internet security technology, provides a broad range of content and network security software and appliance solutions to individuals, enterprises and service providers. The company is a leading provider of virus protection, firewall and virtual private network, vulnerability management, intrusion detection, Internet content and e-mail filtering, remote management technologies and security services to enterprises and service providers around the world. Symantec's Norton brand of consumer security products is a leader in worldwide retail sales and industry awards. Headquartered in Cupertino, Calif., Symantec has worldwide operations in 37 countries.

[www.symantec.com](http://www.symantec.com)

**Mark Your Calendar**  
for  
**Homeland Security**  
**2002**  
**December 9-10**



Renaissance Washington DC Hotel  
Washington, DC



To subscribe to the *E-Gov Digest* and for more information on upcoming events and publications, please visit  
**[www.e-gov.com](http://www.e-gov.com)** or call **800-746-0099**.

# HOMELAND SECURITY 2002: EVOLVING THE HOMELAND DEFENSE INFRASTRUCTURE

Renaissance Washington DC Hotel  
Washington, DC

## Signature Sponsor:

The Oracle logo, featuring the word "ORACLE" in a bold, sans-serif font with a registered trademark symbol.

Oracle Corporation provides the software that powers the Internet.  
[www.oracle.com](http://www.oracle.com)

## SPONSORS

Booz | Allen | Hamilton


[www.bah.com](http://www.bah.com)

**NORTHROP GRUMMAN**  
*Information Technology*


[www.northropgrummanit.com](http://www.northropgrummanit.com)

**zaplet**<sup>TM</sup>

[www.zaplet.com](http://www.zaplet.com)

 symantec.  
The Symantec logo, featuring a stylized circular icon with a gradient and the word "symantec." in a sans-serif font.

[www.symantec.com](http://www.symantec.com)

Homeland Security 2002: Evolving the Homeland Defense Infrastructure  
is an  Conference.

[www.e-gov.com](http://www.e-gov.com)